DOI: 10.19279/TVZ.PD.2014-2-1-14

SUSTAV ZA UPRAVLJANJE I NADZOR RAČUNALNE MREŽE – ZENOSS

Gordan Davidović, Ivan Petričušić, Dubravko Žigman

Tehničko veleučilište u Zagrebu

Sažetak

Rad se bavi problematikom nadzora računalnih mreža na primjeru mreže podatkovnog centra. Nadzor mreže podatkovnog centra izvršen je pomoću Zenoss sustava za nadzor i upravljanje koji SNMP protokolom (eng. Simple Network Management Protocol) komunicira sa ostatkom mrežne infrastrukture. Kako bi se bolje razumio koncept i topologija upravljanja mrežom, prikazana je komunikacija SNMP agenata sa upravljačkom stanicom, te poruke koje oni razmjenjuju. U radu je pokazana i usporedba komercijalnih i besplatnih alata za nadzor, te su iznesene prednosti i mane istih. Ovi sustavi mjere različite performanse mreže i tako otkrivaju moguća „uska grla“ u mreži. Kao što je od kritične važnosti da se prati mreža, od iste takve važnosti je da se dobro odluči što pratiti na mreži. Iz tog razloga je osigurano da topologija korištene mreže bude u skladu s najnovijim tehnologijama.

Ključne riječi: *zenoss, nadzor, SNMP, računalna mreža, podatkovni centar*

Abstract

The master thesis is based on network management using the example of one data center network. Monitoring data center network was made using system Zenoss which communicate with other network equipment by SNMP protocol. For better understanding the concept of network management there is shown how SNMP agents communicate with SNMP managment station, and which messages they exchange. In thesis is also shown comparation of commercial and open-source monitoring tools, and their pros and cons. These systems measure various network performance and thus reveal the possible „bottleneck“ of the system. It is not just important to monitor the network, is is also important to made a decision what resources have bigger priority on the network. For this reason, it is ensured that the topology of the network must be in accordance with the latest technology.

Key words: *zenoss, monitoring, SNMP, network, data center*

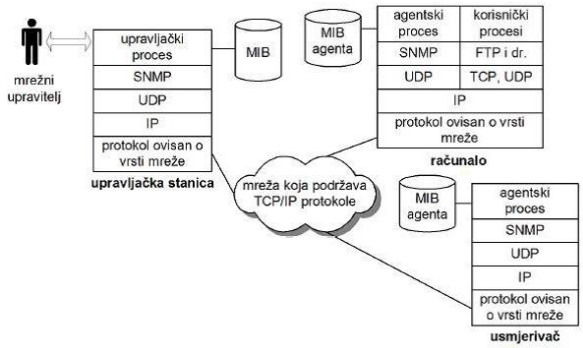
1. UVOD

Brzim razvojem računala i mrežne tehnologije, upravljanje računalnim sustavima postaje sve kompleksniji i vremenski zahtjevniji proces, osobito kada se u obzir uzmu velika korporativna okruženja koja sadrže desetke tisuća upravljivih entiteta – računala, korisničkih računa, mrežnih komponenti, periferije i sl. Upravo zbog brzog razvoja računalne industrije te potrebe za centraliziranim upravljanjem nastala je DMTF (eng. Distributed Management Task Force) organizacija koja se brine o standardima i inicijativama vezanim uz upravljanje u velikim distribuiranim sustavima. Kako bi se omogućilo uspješno nadziranje današnjih mreža, nužno je napraviti dobru strategiju upravljanja. Većina arhitektura za upravljanje mrežom temeljena je na istim principima. Arhitektura tipičnog sustava za upravljanje mrežom (eng. NMS – Network Management System) sastoji se od entiteta za upravljanje, entiteta kojima se upravlja i skupa veza između njih. Entiteti kojima se upravlja često se nazivaju i krajnje točke. Oni su obično računala, poslužitelji i drugi mrežni uređaji (usmjerivači, upravljivi preklopnici, vatrozidovi itd.) koji izvršavaju programe, tzv. agente, koji omogućuju slanje obavijesti prilikom detekcije nekog problema (primjerice ako je zauzeće diskovnog prostora prešlo definiranu kritičnu razinu). Kada entitet za upravljanje ili više njih prime dojavu o problemu oni reagiraju tako da izvedu jednu ili više akcija ovisno o postavkama sustava za upravljanje mrežom. Kako je besplatna programska implementacija Zenoss u današnje vrijeme jedan od najpopularnijih alata za nadzor i upravljanje računalnog sustava, odnosno računalne mreže, izabran je kao temelj ovog diplomskog rada. Alat Zenoss korisnicima može pružiti visoku pouzdanost, a specijalne funkcije poput dojave uzbuna putem SMS poruka zadovoljava i najzahtjevnije računalne okoline koje imaju potrebu za brzom reakcijom na nastali problem. U ovom radu je dan primjer jedne takve

okoline – podatkovnog centra, gdje je reakcija na nepredviđene situacije vezane uz IT opremu jedan od ključnih čimbenika poslovanja. [1]

2. SNMP PROTOKOL

SNMP (eng. Simple Network Management Protocol) je najrasprostranjeniji protokol predviđen za rad na TCP/IP mrežama. Radi se o otvorenom standardu koji je relativno jednostavan no ipak dovoljno fleksibilan da pruži mogućnost kvalitetnog upravljanja velikim brojem različitih tipova uređaja u današnjoj distribuiranoj mrežnoj svakodnevici. SNMP nije samo komunikacijski protokol već definira i kako su podaci koji se nadziru organizirani, pohranjeni i na koji način im se pristupa. Zadatak SNMP protokola je da prikuplja i organizira informacije o stanju računalne mreže, a ujedno je i dio sustava za upravljanje mrežom – NMS (eng. network management system), u ovom slučaju Zenoss-a. NMS je sastavljen od jedne ili više upravljačkih stanica na kojima se izvode upravljačke aplikacije te od nekolicine upravljanih čvorova na kojima se izvode upravljački agenti kao što je prikazano na slici 1. [2]

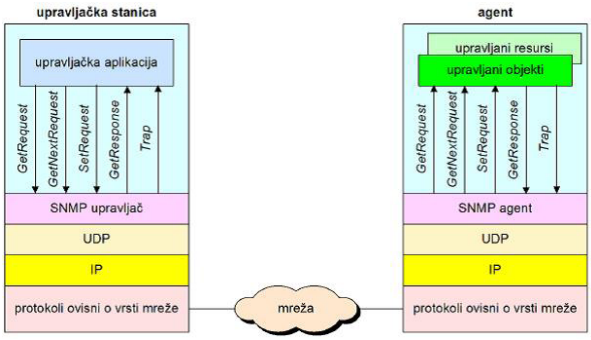


Slika 1. Sustav za upravljanje mrežom u okviru SNMP protokola [1]

Kao što je vidljivo iz slike 1, SNMP protokol služi za povezivanje upravljačkih stanica sa SNMP agentima koji se nalaze instalirani na mrežnoj opremi korisnika, a sve skupa se može objediniti kao usluga za olakšano upravljanje i nadziranje pojedinih dijelova mrežnog sustava na jednom od slijedećih područja:

- upravljanje greškama, tj. otkrivanje i dojava grešaka u sustavu,
- upravljanje konfiguracijom,
- upravljanje performansama,
- upravljanje sigurnošću,
- upravljanje uslugama i
- upravljanje obračunavanjem troškova. [3]

Na slici 2. moguće je vidjeti primjer komunikacije između SNMP agenta i upravljačke stanice, te koje se sve poruke koriste u razmjeni informacija.



Slika 2. Primjer komunikacije SNMP protokola između upravljačke stanice i SNMP agenta [1]

3. RAZVOJ SNMP PROTOKOLA KROZ POVIJEST

U prvoj polovici osamdesetih godina prošlog stoljeća, u mrežama koje koriste TCP/IP protokole nisu bili implementirani protokoli upravljanja mrežnom opremom, već se koristio protokol ICMP (eng. Internet Control Message Protocol). ICMP protokol omogućava prijenos upravljačkih poruka između računala i upravljanih mrežnih uređaja (druga računala, usmjerivači i dr.). Koristeći ICMP i različita zaglavlja IP paketa moguće je razviti jednostavne i moćne alate za upravljanje mrežom (PING, i sl.), no čak ni ti alati ne pružaju dovoljno učinkovitu funkcionalnost za upravljanje složenim mrežama. Stoga je 1987. godine razvijen protokol SGMP (eng. Simple Gateway Monitoring protocol), namijenjen nadzoru usmjerivača. Rastući zahtjevi i brz razvoj tada već složenih TCP/IP mreža, otežavali su mrežno upravljanje. To sve je uvjetovalo daljnji razvoj i poboljšanje protokola SGMP te je time nastao protokol SNMP. IETF (Internet Engineering Task Force) je stvorila SNMP kako bi omogućila upravljanje pomoću normiranog seta operacija, a danas ovaj protokol podržava velika većina računalne opreme, poslužitelja, pisača, preklopnika, vatrozidova, UPS sustava, usmjerivača itd. Od predstavljanja 1988. godine SNMP je postao najpopularniji protokol za upravljanje umreženim računalima i uređajima. Kroz povijest od 1988. godine do danas razvijene su tri inačice tog protokola. [4]

3.1. Snmpv1

SNMPv1 se i danas dosta koristi usprkos poznatim sigurnosnim nedostacima, a prihvaćen je kao standard u TCP/IP mrežama od 1988. godine. Sigurnost se kod SNMPv1 temelji na korištenju takozvanih zajedničkih znakovnih nizova (eng. community string). Community string je u stvari niz tekstualnih ASCII znakova i podsjeća na tradicionalne lozinke koje se koriste u operacijskim sustavima. Koristi se za autentikaciju SNMP poruka između upravljačke jedinice i upravljanog uređaja. Najveći problem je što se ne koristi nikakav oblik enkripcije pa neovlašteni korisnici mogu snimanjem IP paketa koji se prenose mrežom pročitati sadržaj SNMP poruka, a samim time i community string.

3.2. Snmpv2

Verzija SNMPv2 donijela je određena poboljšanja u odnosu na prvu, ali su problemi glede sigurnosti ostali i dalje prisutni. Ova verzija nudi dodatne mogućnosti kao što su sigurnost i autentikacija, a kao standard u mrežama postala je u travnju 1993. godine. Na žalost SNMPv2 nije bio šire prihvaćen jer se IETF nije mogla složiti s pojedinim aspektima sigurnosnih mogućnosti. Zbog toga je 1996. izdana revidirana inačica protokola nazvana SNMPv2c čiji se sigurnosni mehanizam temelji na zajedničkom znakovnom nizu nazvanom community string.

3.3. Snmpv3

Kod SNMPv3 dosta je rađeno na poboljšanju sigurnosnih mehanizama. Posebno treba izdvojiti mehanizme za autentikaciju, tj. provjeru vjerodostojnosti korisnika i zaštitno kodiranje SNMP poruka, odnosno enkripciju. SNMPv3 može koristiti takozvanu korisničku (user-based) autentikaciju (autentikaciju na temelju korisničkog imena i lozinke), a provjera vjerodostojnosti korisnika može se obaviti bez slanja lozinki u čitljivom obliku. [5]

4. USPOREDBA SNMP PROGRAMSKIH IMPLEMENTACIJA

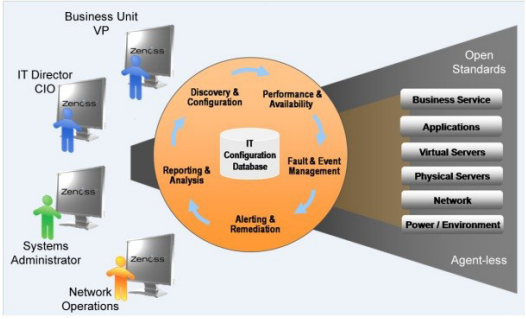
Tablica 1. Usporedba karakteristika programskih implementacija upravljačkih jedinica

	Korisničko sučelje	Komunikacijski protokol	Podržani OS-ovi	SMS dojava	Cijena
HP open view	Aplikacijsko i web sučelje	SNMP+MIB manager	Windows 2000, Server 2003... Unix, Solaris, Linux	Podržava	7000KN
MSC operations manager 2007	Aplikacijsko i web sučelje	SNMP+MIB manager	Windows 2000, Server 2003...	Podržava	7000KN
SNMPc Castle Rock	Lokalna aplikacija / web klijent kao opcija	SNMP, SNMP trap+MIB manager	Windows NT4, 2000, XP, Server 2003, Vista	Podržava	17000KN
Zabbix	Web klijent	SNMP, SNMP trap	*nix	Podržava	Besplatan
Zenoss	Web klijent	SNMP (OID+MIB), Nagios dodatak	*nix	Podržava	Besplatan
Net SNMP	Web sučelje	SNMP	*nix	Ne podržava	Besplatan
OpenNMS	Web klijent	SNMP+MIB manager	Bilo koji OS koji podržava Java	Podržava	Besplatan

5. ZENOSS – O ALATU

Sustav za upravljanje i nadzor računalne mreže (NMS) predstavlja integrirani skup alata koji omogućuju centralizirano upravljanje cjelokupnom IT infrastrukturom nekog poduzeća. Zenoss je jedan od takvih sustava, te je ujedno i jedan od vodećih open-source rješenja za upravljanje i nadzor računalne mreže. Zenoss prati cjelokupnu korisničku fizičku i virtualnu IT infrastrukturu pomoću standardnih protokola kao što su SNMP, WMI i SSH. Prednost Zenoss-a nad drugim alatima je u tome što je besplatan, jednostavan za instalaciju i primjenu, a nedostatak je taj što korisnička podrška nije tako dobra kao kod komercijalnih alata (HP Open View, MSC operations manager...).
Kao što je moguće vidjeti iz slike ispod, osnovne funkcionalnosti Zenoss-a su:

- Otkrivanje i konfiguracija uređaja
- Provjera dostupnosti uređaja i performanse
- Upravljanje greškama i događajima
- Upozoravanje i sanacija grešaka
- Izvještavanje i analiza [6]

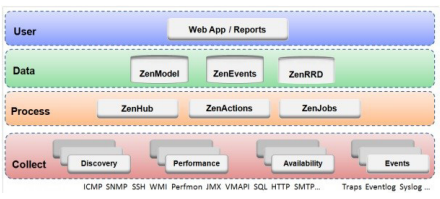


Slika 3. Zenoss [6]

6. ARHITEKTURA ZENOSS-A

Zenoss je slojevit sustav koji se sastoji od 4 glavna dijela:

- Sloj korisnika
- Sloj podataka
- Sloj obrade
- Sloj prikupljanja



Slika 4. Zenoss arhitektura [7]

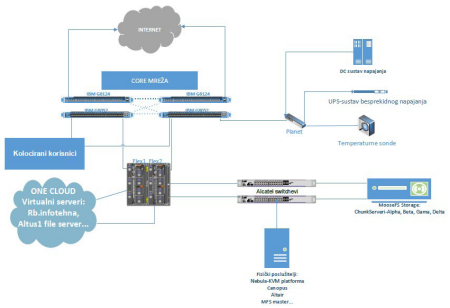
Korisnički sloj je građen oko Zope Web aplikacijskog okruženja, te se manifestira kao web portal. Kroz korisničko sučelje moguće je pristupiti i upravljati ključnim komponentama sustava.
Sloj podataka koristi tri baze podataka gdje se pohranjuju informacije:

- ZenRRD – koristi RRDtool, pohranjuje informacije o performansama unutar određenog vremenskog perioda
- ZenModel – sadrži podatke o uređajima unutar MySQL baze podataka
- ZenEvents – sadrži podatke o događajima unutar MySQL baze podataka

Sloj obrade upravlja komunikacijom između sloja podataka i sloja prikupljanja. Periodički obavlja poslove u pozadini, kao i poslove inicirane od strane korisnika.
Sloj prikupljanja sadrži usluge koje prikupljaju podatke i šalju ih sloju podataka. Na temelju njih se vrši modeliranje, nadgledanje i upravljanje događajima. [7]

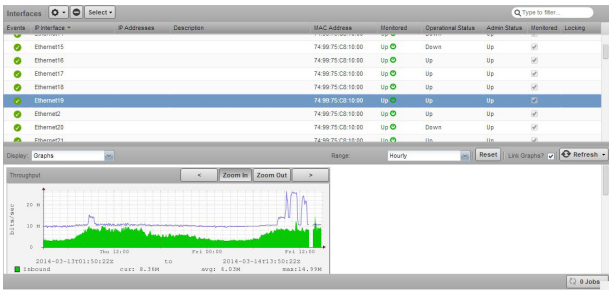
7. PRIMJER KORIŠTENJA ZENOSS SUSTAVA

Kako bi se naglasile sve bitne karakteristike Zenoss sustava, u primjeru je implementiran unutar podatkovnog centra kao alat za kontrolu raznih fizičkih i virtualnih servera, preklopnika, senzora temperature i sl. Zenoss u podatkovnom centru ima ulogu centralnog sustava za nadzor i upravljanje koji je SNMP protokolom povezan sa SNMP agentima koji su instalirani na uređajima koji se prate. U ovom slučaju prate se svi mrežni uređaji jer su u produkcijskom stanju, te je vrlo bitno da mrežni administrator zna za svaki događaj vezan uz svaki pojedini uređaj. Na slici ispod moguće je vidjeti shemu mreže podatkovnog centra, čije upravljanje je detaljno opisano u radu:



Slika 5. Shema mreže podatkovnog centra

Instalacija Zenoss-a unutar podatkovnog centra izvršena je na zasebnom virtualnom poslužitelju (na shemi „ONE CLOUD“). Instalacija je izvršena na virtualnom poslužitelju radi eventualne lakše migracije na drugi fizički „node“ ukoliko dođe do nekih problema, te radi lakšeg backupiranja cijelog sustava koji se redovno vrši nad svim virtualnim poslužiteljima. Dodavanje i klasifikacija uređaja unutar Zenoss sustava vrši se vrlo jednostavno uz pretpostavku da je na uređaju instaliran SNMP agent (ukoliko nije, potrebno ga je instalirati). Komunikacija između centralnog sustava i SNMP agenata uspostavljena je pomoću SNMP protokola verzije 2c. Pošto je unutar podatkovnog centra brzina reakcija ključan čimbenik, unutar Zenoss-a su postavljene razne granice (iskorištenje procesora, memorije, stupanj temperature...) za servere i ostalu mrežnu opremu, te ukoliko dođe do nekog incidenta, korisnicima se šalju upozorenja putem SMS-a i e-maila. Kako bi korisnici mogli dobiti samo one najbitnije informacije o uređajima, iste je moguće modelirati po željama. Još jedna od bitnih stvari su izvještaji o uređajima, događajima i sl., a koji služe kao vjerodostojan prikaz svih zbivanja u korisničkoj IT infrastrukturi, te je na temelju njih moguće donositi odluke vezane uz kupovinu nove opreme, zamjenu stare opreme za novu i sl. Jedna od glavnih karakteristika Zenoss-a je preglednost, pa je tako moguće pregledavati razne vrste grafova, te ih čak ručno kreirati po vlastitim željama. Primjer grafa na kojemu se vidi ukupan mrežni promet (Mbit/sec) unutar određenog vremenskog razdoblja pokazan je na slici ispod.



Slika 6. Primjer grafa (količina mrežnog prometa/određeni vremenski period)

8. ZAKLJUČAK

SNMP protokol je dizajniran da minimizira složenost i broj upravljačkih funkcija realiziranih od agenata, a da opet bude fleksibilan kako bi se mogao prilagoditi nepredvidljivim aspektima mrežnih operacija nadzora i upravljanja. Glavni aduti SNMP-a su jednostavnost i interoperabilnost. Njegova važna odlika je da SNMP mora efektivno raditi i kada mreža nije potpuno operabilna. To se odražava u izboru nespojnog transportnog protokola (UDP) koji dopušta upravljačkim aplikacijama potpunu kontrolu nad mehanizmom retransmisije, a što je vrlo bitno kod nadzora i upravljanja računalnim mrežama podatkovnih centara. Upravljanje mrežnim sustavima danas je sveprisutno i neophodno u gotovo svim svjetskim organizacijama. Kao jedan od vodećih sustava za nadgledanje mreže i mrežnog prometa nameće se besplatna programska implementacija pod nazivom Zenoss. Zenoss korisnicima omogućava jednostavnu, ali intuitivnu interakciju sa svim bitnim resursima mrežnog sustava, te povećava sigurnost IT mreže za 50%.

9. LITERATURA

[1] CARNet Hrvatska akademska i istraživačka mreža, NCERT-PUB-DOC-2010-09-313: „SNMP protokol“

[2] Bruey, Douglas: "SNMP: Simple Network Management Protocol", Rane Corporation, 2005.

[3] Bažent, Alen: "Osnove arhitekture mreže", Element Zagreb, 2003.

[4] Mauro, R. Douglas; Schmidt, Kevin James: "Essential SNMP: Simple Network Management Protocol ", O'Reilly Vlg. GmbH & Company, 2001

[5] Runac, Neven: "Sigurnost SNMP protokola", SRCE Zagreb, 2009.

[6] Monitoring Zenoss, s Interneta, http://security.foi.hr/wiki/index.php/Monitoring_-_ZenOSS, 07.04.2014

[7] Williams K., Gareth; Torvalds, Linus: "Zenoss Service Dynamics Resource Management Administration", Zenoss, 2013, 193 stranice

AUTORI

Gordan Davidović. Rođen sam 21.11.2014 u Zagrebu gdje sam proveo djetinjstvo. Nakon završene osnovne škole „Vladimir Nazor“ pohađao sam XV. Gimnaziju u Zagrebu informatičkog smjera. Diplomirao sam smjer telekomunikacije na „Fakultetu elektrotehnike i računarstva“ u Zagrebu. Po završetku studija, nastavljam obrazovanje na Cisco akademiji Tehničkog veleučilišta u Zagrebu (TVZ), te radim kao sistemski inženjer u tvrtki „Combis“. 2008. godine prelazim u tvrtku „VIPnet“ na radno mjesto višeg specijalista za poslovna rješenja, te počinjem predavati na Cisco akademiji TVZ-a. Dvije godine kasnije, postajem vanjski suradnik (asistent) TVZ-a.

Ivan Petričušić rodio se u Bjelovaru 20. prosinca 1987. godine. Tehničku školu Bjelovar završava 2006. godine, te nakon toga, 2007. godine upisuje preddiplomski stručni studij na Tehničkom veleučilištu u Zagrebu. Studij završava 2010. godine, te stiče titulu bacc. Ing. Računalstva. Paralelno sa studijem upisuje CCNA cisco akademiju, te ju završava u prvom mjesecu 2010. godine. Iste godine upisuje specijalistički diplomski stručni studij informatike na Tehničkom veleučilištu u Zagrebu, te ga završava u 4. mjesecu 2014. Radi kao sistem administrator u podatkovnom centru Altus informacijske tehnologije gdje stječe iskustvo radom na raznim projektima vezanim uz „core networking“ i infrastrukturu podatkovnog centra.

Mr. sc. Dubravko Žigman rođen je 1970. godine u Zagrebu, gdje završava osnovnu školu i srednju matematičku školu. Studij završava 1996. godine na smjeru Elektroenergetika, usmjerenju Opća energetika. 2002. godine stiče stručni naziv magistra znanosti iz polja Elektrotehnike, smjer Elektroenergetika. Od 2006. radi na TVZ-u kao viši predavač. Dobitnik je slijedećih nagrada: 2013 nagrada u kategoriji CCNP Curricula Excellence, 2008 dobitnik tri od četiri priznanja koje dodjeljuje Cisco: Education Recognition, Extraordinary Contributions i Pioneer Recognition. 2005 NetAkademija proglašena za najbolju lokalnu Cisco akademiju u EMEA regiji. Nositelj je nekoliko priznatih industrijskih certifikata: CompTIA A+, MCP, CCNA, CCAI, CCNP, NLP-Practitioner IANLP.